3. GETTING CONTROL OF THE PROBLEM — KEEPING YOUR OWN AGENCY RUNNING

If your emergency response agencies are at risk from Y2K problems, you need to plan ahead in order to keep operating if they strike. That's the only way you'll be able to help your communities.

Keep in mind that the Y2K problem could affect both computers and computer-driven products or systems. It could also affect many electronic devices that are common in emergency management. Remember — check all devices and systems that could be affected by the Y2K problem.

How Will I Know If My Own Systems Are Y2K Compliant?

NOTE: This guide does not give detailed instructions for testing systems for Y2K compliance. Instructions and tools are available on many State and commercial web sites. A partial list appears later in this section.

You cannot test your systems by just setting your computer's clock to 11:59 PM, December 31, 1999, and waiting 1 minute to see what happens. Problems may exist on many different levels, so you must ensure that all technology levels of your systems are Y2K compliant. Check with vendors and other experts to ensure Y2K compliance.

❑ Check Your Hardware

This task should cover both the specific chip architecture and the machine's internal clock. Check the web sites or user support lines of your hardware vendor and your operating system vendor for Y2K issues. Use either firmware changes from the hardware vendor or operating system patches.

❑ Check Your Operating System

Even some recent operating systems require upgrades to be fully Y2K compliant. Check your vendor's web site or user support line for Y2K issues.

❑ Check Your Databases and Files

These include all of the files and data used by your applications. Dates can be stored in any of your databases. Check to ensure their data management system is Y2K compliant. Also ensure that any custom date usage is based on 4-digit years or that you have a clear method for processing 2-digit years stored in custom date fields.

❑ Check Your Applications and Run-Time Libraries

Applications software runs on your operating system and works with various databases. Ensure that all applications you use and their run-time libraries are Y2K compliant. Check your application vendor's web site or user support line for Y2K issues.

❑ Check Your Custom Code

Custom applications are either built on top of application software or use application software components. Even though the underlying applications are Y2K compliant, the custom code may not be. Establish guidelines for testing your code to ensure that it is Y2K compliant. Accept only Y2K-certified applications from third-party developers.

Resources for Testing Your Systems

Many web sites list testing procedures and have software tools available for testing your systems. For example, see the following:

http://y2k.state.wi.us/
http://www.usfa.fema.gov/
http://www.nist.gov/

The web sites of many States also provide information, tools, and links to other web sites. The information on these sites and elsewhere is highly technical because the problem is complicated. You may need the help of an IT expert to solve it.

Where Can I Get Help in Fixing My Systems?

Many of the same sources listed for testing your systems also have software available for repairing some problems. Hardware and software vendors' web sites may have updates that you can use to fix their particular products.

Many service providers can help fix your systems, but FEMA cannot endorse specific private firms. You may be able to get help or advice on private firms from your State's information technology staff.

You can also locate resource lists of service providers on the World Wide Web by doing a keyword search. Try using search terms such as "Year 2000" or "Y2K."

Planning for Continuity of Operations

Even if you've tried to ensure that all your systems are Y2K compliant, you may suffer some unexpected failures. So plan ahead to keep your agency running and able to provide service in case of system failures.

In this regard, you're like any other agency or commercial business. So the guidance that has been written for them is good for you, too. There's extensive guidance on operations continuity planning in the web sites and publications listed in *Section 5*. To get you started, here's a step-by-step process taken from the General Accounting Office, *Year 2000 Computing Crisis: Business Continuity and Contingency Planning*, GAO/AIMD-10.1.19, August 1998. For a complete copy, see http://www.gao.gov/special.pubs/bcpguide.pdf

The following steps will help you plan for continuity of operations.

Steps for Continuity Planning

Step 1. Initiation

- ❑ Establish an operations continuity project work group
- ❑ Develop and document a high-level operations continuity planning strategy
- ❑ Identify core processes for operations
- ❑ Define roles and assign responsibilities
- ❑ Develop a master schedule and milestones
- ❑ Implement a risk management process and establish a reporting system
- ❑ Assess existing continuity, contingency, and disaster recovery plans and capabilities for core operations
- ❑ Implement quality assurance reviews

Step 2. Operations Impact Analysis

- ❑ Define and document information requirements, methods, and techniques to be used in developing the operations continuity plan
- ❑ Define and document Year 2000 failure scenarios
- ❑ Perform risk and impact analyses of each core operations process
- ❑ Assess and document infrastructure risks
- ❑ Define the minimum acceptable level of outputs and services for each core operations process

Step 3. Contingency Planning

- ❑ Assess the cost and benefits of identified alternatives and select the best contingency strategy for each core operations process
- ❑ Identify and document contingency plans and implementation modes
- ❑ Define and document triggers for activating contingency plans
- ❑ Establish a resumption team for each core operations process
- ❑ Develop and document a zero day strategy and procedures

Step 4. Testing

- ❑ Validate your operations continuity strategy
- ❑ Develop and document contingency test plans
- ❑ Establish test teams and acquire contingency resources
- ❑ Prepare for and execute tests
- ❑ Validate the capability of contingency plans
- ❑ Rehearse operations resumption teams
- ❑ Update the continuity plan based on lessons learned and re-test if necessary
- ❑ Update disaster recovery plans and procedures